WHAT IS CLAIMED IS:

1. A method of processing a packet having a plurality of layers, comprising:

processing a first layer in accordance with a first protocol; and

processing a second layer in accordance with a second protocol in parallel with processing of said first layer when processing of said first layers uncovers sufficient information to support processing of said second layer.

2. A method of processing a data packet according to a plurality of security policies, comprising the steps of:

(a) receiving the packet;

(b) identifying a first security policy;

(c) processing the packet according to the first security policy;

(d) identifying a second security policy when information necessary for said identification of the second security policy becomes available; and

(e) processing the packet according to the second security policy, concurrently with step (c).

3. The method of claim 2, wherein said step (c) comprises decryption of data in the packet.

4. The method of claim 3, wherein said decryption is performed according to the data encryption standard (DES).

5. The method of claim 3, wherein said decryption is performed according to the triple data encryption standard (3DES).

6. The method of claim 3, wherein said decryption is performed according to the ARC4 algorithm.

7. The method of claim 2, wherein said step (e) comprises decryption of data in the packet.

8. The method of claim 7, wherein said decryption is performed according to the DES.

9. The method of claim 7, wherein said decryption is performed according to the 3DES.

10. The method of claim 7, wherein said decryption is performed according to the ARC4 standard.

11. The method of claim 2, wherein said step (e) comprises authentication of the data packet.

12. The method of claim 11, wherein said authentication comprises application of the Multilayer Modular Hashing (MMH) algorithm.

13. The method of claim 11, wherein said authentication comprises application of the Hash-based Message Authentication Code (HMAC) Secure Hash Algorithm (SHA)-1.

14. The method of claim 2, wherein said step (e) comprises re-encryption of decrypted data from the packet.

15. The method of claim 14, wherein said re-encryption comprises encryption performed according to the Advanced Encryption Standard (AES).

16. A system for processing a data packet according to a plurality of security policies, wherein processes that effect respective security policies can execute in parallel, the system comprising:

a packet identification (PID) parser that identifies the packet;

a plurality of security processing modules, each of which can process the packet according to one of the security policies in parallel with at least one other security processing module; and

at least one feedback loop or feeding output of at least one of said security processing modules to at least one other security processing module.

17. The system of claim 16, wherein said security processing modules comprise a module for performing decryption according to the DES.

18. The system of claim 16, wherein said security processing modules comprise a module for performing decryption according to the 3DES.

19. The method of claim16, wherein said security processing modules comprise a module for performing Digital Video Broadcast (DVB) descrambling.

20. The system of claim 13, wherein said security processing modules comprise a module for performing HMAC authentication.